BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

AD

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 843 449 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.05.1998 Bulletin 1998/21

(51) Int. Cl.[6]: **H04L 29/06**

(21) Application number: **97119539.1**

(22) Date of filing: **07.11.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **08.11.1996 US 744430**

(71) Applicant:
Sunhawk Corporation, Inc.
Seattle, Washington 98112 (US)

(72) Inventors:
- **Eller, Marlin J.**
  Seattle, Washington 98112 (US)
- **Mills, Brent R.**
  Seattle, Washington 98115 (US)

(74) Representative:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Encryption system with transaction coded decryption key

(57) The encryption secured computer system (10) includes a server (12) that communicates with clients (14-20) across a public network (21) using a novel transaction coded decryption key technology that discourages wrongful redistribution of protected information such as digital musical scores, and allows for tracking of infringing activity. In one implementation, the server (12) distributes access software and partially encrypted musical scores to clients upon request. A client can sample the partially encrypted scores prior to consummating a transaction. When a score is selected, the client enters payment information and is assigned a password that is specific to the client and transaction. The password functions as a decryption key to enable use of the musical score by the client employing the access software. Any subsequent wrongful redistribution of the musical score together with the decryption password can be traced due to client identifying information encoded into the password.

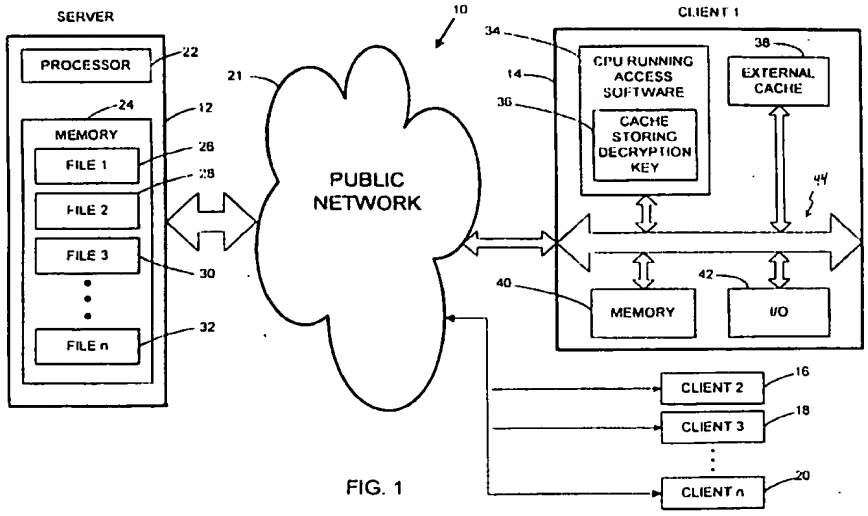

FIG. 1

EP 0 843 449 A2

desired to monitor the distribution of proprietary subject matter over a public network. In the following description, the invention is set forth in the context of monitoring distribution of digital musical scores over a network. It will be appreciated that this particular application is set forth for the purpose of illustrating the invention, and various aspects of the invention have broader application as defined by the claims below.

Fig. 1 illustrates an encryption secured computer system 10 according to the present invention. The computer system 10 includes a server 12 that can communicate with clients 14-20 across a public network 21 such as the Internet. In the case of the Internet, the server 12 can be accessed via the Netscape 2.01 or Microsoft Internet Explorer 3.0, or higher browsers. The server 12 generally includes a processor 22 and a library or database of digital musical scores stored in a memory 24 as files 26-32. As discussed in detail below, the server 12 is operative for receiving access requests from clients 14-20, assigning decryption keys or passwords and transmitting an accessing program and selected scores to the clients 14-20 over network 21. A number of other functions relating to receiving payment, indexing and storing encoded decryption passwords and the like are also performed by server 12.

For present purposes, the clients 14-20 may be considered as being functionally equivalent. Details of only one of the clients 14 are shown in Fig. 1. Generally, the client 14 includes a central processing unit (CPU) 34, an internal cache 36 and/or external cache 38, memory 40 and input/output (I/O) hardware 42, all interconnected via data bus 44. The CPU, which may include any suitable microprocessor, is operative for downloading and running the accessing program. accessing memory 40 and caches 36 and 38, and communicating with I/O hardware 42. In the illustrated embodiment, the CPU 34 also includes a built-in, internal cache for storing the decryption key used to decrypt downloaded musical scores. Generally, cache 36 is an area of extremely fast Random Access Memory (RAM) for storing frequently used or time critical data so as to allow for faster operation. The cache 36 can be accessed more rapidly than memory 40. Alternatively, the decrypting key can be stored in an external cache 38, which may comprise a RAM chip located on the computer motherboard. Memory 40, which is separate from caches 36 and 38, may include computer memory as well as the storage of floppy disks, CD-ROM drives and hard drives. The I/O hardware 42 can include a number of types of devices including a mouse, keyboard or other user input device; a viewing monitor; a printer; or a MIDI device.

Fig. 2 provides a functional overview of a music distribution monitoring system 46 used in connection with the computer system 10 of Fig. 1. As shown in Fig. 2, the monitoring system 46 can be broken down into a number of functions that are executed by logic on the server and/or a client. The functions of the illustrated system 10 include: downloading (48) a music accessing program, in this case designated the "Music Viewer," for use by a client in accessing music files stored on the server; downloading (50) a selected musical score from the server; purchasing (52) music on-line (and thereby obtaining an access license and encoded decryption key); printing (54) and/or viewing (56) the music and music encryption/decryption. It will be appreciated that the music may also be reproduced from digital information using a MIDI device or the like. Each of these functions is discussed in turn below.

Fig. 3 illustrates the Music Viewer download function of one implementation of the present invention. After communication between the server and client has been established through the network, the client initiates the download function by requesting (58) the server to download the program. This request can be entered by following appropriate prompts from the server site. The server receives (60) the download request and sends (62) the Viewer software package to the client. Upon receiving (64) the software package, the client runs the setup code to install the Music Viewer software. In order to access musical scores stored in the server library in the illustrated system, the client is assigned a unique Viewer identification code. Accordingly, the client is prompted to request (66) a Viewer ID as part of the download procedure. In response to the ID request, the server generates (68) a Viewer ID and logs the ID in a Viewer database. The server then sends (70) the newly generated Viewer ID to the client and logs the transmission time and date, the Internet Protocol (IP) address (or similar information for other networks) of the client, and the client's machine name or type (as entered by the client user or determined from a transmission header or the like). The client then receives (72) the assigned Viewer ID and a successful installation is thus completed.

The system of the illustrated embodiment allows the client user to browse through the music library and view a selected portion, e.g., the first page, of musical scores prior to consummating a transaction by purchasing a music copy or paying a license fee. Fig. 4 illustrates the associated pre-purchase music download function. The function is initiated when the client selects a score to sample and requests (74) the music from the server. In this regard, the score may be selected from a list of titles by scrolling through the library and clicking on a selected title, by using a search function to call a title, or by any other appropriate means. The Viewer ID is also sent to the server at this time. Upon receiving the request, the server finds (76) the requested musical score, compresses and encrypts (or partially encrypts) the score as will be described below, and stores the encrypted score in the download area. In addition, the server assigns and logs a decryption key that is unique to the client and also logs an identification code for the score, the download IP, and the Viewer ID for the transmission. For example, the key can be a password com-

posed of two 32 bit numbers where one of the numbers is an index to identify the client in a client database and the other number is random, or encoded with additional information as desired. By indexing the key or password to the client database in this manner, the password can be used to identify the client, look up license or account information and otherwise monitor distribution on a client-specific and transaction-specific basis.

The server then sends (78) the client the Uniform Resource Locator (URL) address of the newly encrypted music. Upon receiving (80) the URL, the client can request (82) a download of the file or files containing the encrypted music. The server then finds (84) the encrypted music in the download area, queues up the music, and downloads (86) the music to the client. The client receives (88) the encrypted music and stores the music in memory, e.g., computer memory, hard drive storage. etc. At this point in the illustrated implementation, i.e., prior to purchase, only the first page of the score is not encrypted. Accordingly, the client user can play and view (90) the first page of the music to verify that the downloaded score is the score desired by the user and to otherwise evaluate purchasing options.

After thus browsing through the music library and sampling one or more scores, the client user may decide to make an on-line music purchase, e.g., to purchase a copy of the music in sheet music form, or to pay a license fee to print copies, view the music in its entirety, play back the music on the client's I/O hardware, or otherwise use the music. Such a license may be for single use, multiple use, unlimited use during a license term, etc. Fig. 5 illustrates the on-line purchase function. The function is initiated by the client by sending (92) payment information (for example, a credit card account number and expiration date, or the number of a previously established, pre-paid or unpre-paid account with the server institution), the score ID, the download IP, Viewer ID and/or any other information to the server. Some or all of this information may have already been transmitted to the server in connection with browsing the music library and would not necessarily have to be retransmitted. The exchange of personal and financial information can be encrypted using standard public key encryption as provided, for example, in the Secure Sockets layer of the browser.

Upon receiving (94) this information, the server downloads the score and Viewer ID, and contacts the client user's financial institution or a credit card approval service, looks up balance information, or otherwise obtains authorization for the transaction. Based on the results of this authorization inquiry, the server sends back (96) to the client either a bad payment message (e.g, "payment declined'), or the server sends a decryption password and logs the password and other transaction information in its database. By operation of the Music Viewer software, the client then receives (98) the password and stores the password in a password database separate from the downloaded music. It will thus be difficult for a client user to improperly redistribute music because the user will generally not be aware that a decryption password has been stored in its system, nor will the user know how to access the password. In operation, the Music Viewer software monitors client messages until it receives (100) an "open file" message indicating that the user desires to print, playback or otherwise use the music. At this time, the Music Viewer locates (102) the password, which may be stored in a client cache for speed of operation. The Music Viewer can also retrieve license information relevant to the client's access request and, in appropriate cases, increment the client use count under the license as discussed below. If the client has remaining uses under a license, the Music Viewer decrypts the score in memory. It will be noted that the music is never saved in decrypted form, but is only decrypted just-in-time for a requested use, thereby discouraging improper redistribution.

Fig. 6 illustrates a music printing function according to the invention. As previously noted, after downloading music and a password, the Music Viewer monitors client messages to identify access requests. When a print command is received (104), the Music Viewer consults its client database to determine (106) whether there are any remaining printouts allowed under the license previously purchased by the client user. In this regard, the client user may have payed a single use or multi-use license fee. If the license has been exhausted, the client is notified (108) accordingly, and information may be provided concerning options for paying a further license fee. Otherwise, the Music Viewer encodes (110) various information regarding the transaction in the user database, e.g., Viewer ID, score ID, download ID, date, time and number of licensed printouts used. This information can be encoded, for example, in a base 72 number string in an appropriate format, and then printed (112) on the copy (e.g., next to the copyright notice). Similarly, this same identification information can be written into a comment statement of a MIDI file to tag MIDI extractions. This information allows for proper incrementing of a multi-use license and also allows for subsequent tracking of any improper redistribution of the printed copy. In this regard, if a printed copy of the score or MIDI file is found, the associated transaction and client can be readily decoded.

Instead of, or in addition to printing the music, the on-line user may desire to view the music on a monitor. For example, the music may be viewed in conjunction with playing back the music for enhanced enjoyment, or the music may be displayed to facilitate selection of playback options involving tempo, instrumentation and the like. Fig. 7 illustrates the associated music viewing function. Upon receiving (114) a display command, the Music Viewer opens (116) the requested music file and determines (118) whether the file is encrypted. If the music is not encrypted, e.g., because it has been decrypted in a previous step or is public domain music,

the music can be directly displayed (124). However, in the case where the music is encrypted with the exception of the first page for sampling, the Music Viewer proceeds to display (120) the first page and disable printing or MIDI extraction. If the client user then attempts to display the remainder of the music, the Music Viewer first determines (122) whether a valid and unexpired password has been assigned to the user. If so, the music is decrypted and displayed (124). Otherwise, an error message is displayed (126).

Figs. 8 and 9 illustrate one implementation of the encryption/decryption function of the music distribution monitoring system. It will be appreciated that any suitable technique, including using a public key encryption/decryption algorithm, can be employed as the base level encryption/decryption technology in accordance with the present invention. In addition, the base level encryption/decryption technology can be implemented in hardware and/or software logic. The following description illustrates one exemplary implementation. Referring first to Fig. 8, the encryption/decryption components are schematically shown. On the server side, the encryption/decryption subsystem 126 includes compression logic 128, random number generator 130 and exclusive OR (XOR) gate 132. The compression, which can be a conventional data compression software program or a data compression hardware package, receives the raw digital musical score and compresses the score for transmission. It will be appreciated that this compression. in addition to improving transmission speed, enhances subsequent encryption as the compressed and encrypted data will be especially difficult for an intercepting party to decipher. The random number generator 130 can include one or more conventional random number generating programs. In this regard, two such programs can be employed to handle the two 32 bit words of the decryption password. The random number generator 130 implements an algorithm for generating a determined series of values starting from an initial seed. In the illustrated embodiment, the assigned password is provided to the generator 130 as a seed. The generator 130 also receives an input from the compressed data stream line that triggers the generator 130 such that the generator 130 outputs a bit stream equal in length to and coordinated with the compressed data stream. The generator output and compressed data stream are used as the two inputs into the XOR gate 132 which performs its characteristic disjunctive comparator function. The output from XOR gate 132 is transmitted over the network to the client.

On the client side, the subsystem 126 includes a client-side random number generator 134 and client-side XOR gate 136, each identical to its server-side counterpart. Th- subsystem 126 further includes decompression logic 138 that is the logical complement of compression logic 128. The random number generator 134 uses the password as a seed, and generates a bit stream of length determined by an input from the encrypted data stream. It will thus be appreciated that the output bit stream from generator 134 will be identical to that of generator 132, this output, and the encrypted data stream, serve as the two inputs into XOR gate 136. The successive operation of the XOR gates 132 and 136 yield an output from XOR gate 136 that is identical to the output from compression logic 128, i.e., a compressed digital music score. This compressed score is decompressed by decompression logic 138 to yield the digital score in uncompressed, decrypted form. It should be noted that the musical score is decrypted as part of the music output process, not prior to saving the score. Additionally the encryption/decryption process can be successively performed on page-sized chunks in the case of printing, or on appropriately-sized portions of an audio output (e.g., two seconds of the score), in order to allow for display/play-back on an as-ready basis.

The encryption/decryption process is summarized in the flow chart of Fig. 9. The process is initiated, on the server side, by receiving (140), or calling from memory, a digital representation of the musical score. The digital representation is then, in sequence, compressed (142), encrypted (144) and transmitted (146) across the network to the client. On the client side, the signal is first decrypted (148) to obtain a compressed digital representation, and then decompressed (150) to obtain the digital score. The score can then be output (152) as desired by the client user.

The following prophetic example illustrates the overall operation of the music distribution monitoring system of the present invention. A client accesses the music distribution server at its World Wide Web site using, for example, the Microsoft Internet Explorer 3.0 browser. From the server home page, the user first selects the option for downloading the Music Viewer program. After selecting this option, the user follows the prompts or instructions to install the software and, in the process, enters various requested identification data. The user may then return to the home page and select the music library option to browse the available selections. The user can then scroll through the available selections to identify a score of interest, for example, "Mozart's Sonata Number 1." In order to verify that this is the piece that the user has in mind, the user may download the score for sampling. The Music Viewer software stores the partially encrypted digital score and will allow the first page of the score (which is transmitted in unencrypted form) to be displayed on the client monitor and played back.

After one or more scores are thus sampled, the user may decide that he desires to print, view or otherwise use a digital score and that he therefore desires to purchase a copy of or pay a license fee for the score. The user can then select a purchase function and a menu of purchase options will be provided, e.g.. single print license multi-print license, unlimited viewing license for a given license term, etc. The user selects

the desired option, responds to a series of prompts concerning identification information and payment information, e.g., by entering a credit card number and personal information. If payment is approved, the user will be assigned a decryption password that is indexed to the client's identifying information in a client database held by the server. By way of example, the client may pay a license fee for ten printouts. In the same or subsequent sessions, the client can request a printout under the license. The system will keep track of the number of printouts used and allow printing only so long as the license is unexhausted. Whenever the user prints out a copy of the score, an encoded string of characters is printed next to the copyright notice.

An unscrupulous user may attempt to redistribute the music with disregard for the server/copyright holder's rights. Having the downloaded music file on his system, the user may attempt to redistribute the music electronically. However, having thus attempted to wrongfully redistribute the music, the user will discover that the redistributed information cannot be used because it is encrypted. Such a user may attempt to break the encryption code and may even ultimately surmise that a key has been stored in the client's memory somewhere separate from the music file. In the unlikely event that the user should succeed in redistributing the music together with the password in useable form, the infringing user will have unwittingly left a record of his infringing activity in the form of the personal information that can be derived from the client/transaction encoded password. Similarly, redistribution of printed copies or MIDI files will provide a record due to the coded character string included with the copyright notice or in comment statements. In any event, the coded information facilitates enforcement and thus discourages infringement.

While various embodiments and applications of the present invention have been described in detail, it is apparent that further modifications and adaptations of the invention will occur to those skilled in the art. However, it is to be expressly understood that such modifications and adaptations are within the spirit and scope of the present invention.

Claims

1. A method for use in monitoring distribution of information accessible through a public network said information included in a database at a server of said public network, comprising the steps of:

   encrypting at least a first portion of said information using a key-based encryption system, said key-based encryption system requiring entry of a key to decrypt said encrypted information;

   in connection with a request by a network client, assigning a first client-specific key to said client for decrypting said encrypted information, said first client-specific key including at least a first identifier useful for identifying said client; and

   transmitting said first client-specific key to said client, wherein said key can be used to monitor distribution of said information on a client-specific basis.

2. A method as set forth in claim 1 wherein said information comprises a digital musical score and said step of encrypting at least a portion of said information comprises retaining a second portion of said digital musical score in an unencrypted form so as to allow for sampling of said digital musical score prior to decryption.

3. A method as set forth in claim 1 wherein said step of assigning said first client-specific key comprises acquiring identification information regarding said client and encoding said identifier with respect to said acquired identification information.

4. A method as set forth in claim 3 wherein said identifier comprises a password that is indexed to a client database including said identification information.

5. A method as set forth in claim 3 wherein said identifier includes information for identifying client equipment.

6. A method as set forth in claim 3 wherein said identifier includes information for identifying a client user.

7. A method as set forth in claim 1, further comprising the step of transmitting said encrypted information to said client prior to said step of transmitting said first client-specific key.

8. A method as set forth in claim 1, further comprising the step of transmitting accessing software to a client, said accessing software being operative for allowing said client to access said information in said database.

9. A method as set forth in claim 8, further comprising the step of employing said accessing software to print a copy of said information.

10. A method as set forth in claim 8 wherein said information comprises a digital representation of a musical score, and said method further comprises the step of employing said accessing software to play back said musical score.

11. A method as set forth in claim 8, farther comprising

the step of displaying said information.

12. A method as set forth in claim 1 wherein said step of assigning said first client-specific key is conducted in response to receiving said request by said client.

13. A method as set forth in claim 1, further comprising the steps of storing said information in a first area of memory and storing said first key in a second area of memory separate from said first area, wherein said information and said first key can be separately accessed.

14. A method as set forth in claim 1, further comprising the steps of storing said information in a client memory in encrypted form, receiving a request to output said information, and decrypting said encrypted information in response to said output request.

15. A method as set forth in claim 1, further comprising the steps of receiving an access request from a second network client requesting access to said information and assigning a second client-specific key, different from said first client-specific key, to said second client for decrypting said encrypted information.

16. A method as set forth in claim 1, further comprising the step of using said first client-specific key to track subsequent redistribution of said information.

17. A method as set forth in claim 1, further comprising the steps of outputting an output copy of said information and embedding identification information in said output copy, wherein said identification information facilitates tracking of redistribution of said information.

18. A computer system for use in monitoring distribution of protected information accessible through a public network, comprising:

a first area of memory tor storing a database including said protected information;
a controller operative for receiving an access request from a network client requesting access to said protected information, obtaining identification information useful for identifying a source, and assigning a decryption key using said identification information; and
encryption logic for encrypting said protected information based on said decryption key wherein said decryption key is useful for decrypting said encrypted protected information.

19. A computer system as set forth in claim 18, further comprising a second area of memory for storing said identification information, wherein said identification information is indexed to said decryption key.

20. A system as set forth in claim 18 or 19 wherein said controller is further operative for receiving payment information from a client, wherein said decryption key is assigned in response to receiving said payment information.

21. A system as set forth in claim 18, 19, or 20 wherein said protected information comprises a digital musical score and said encryption logic is operative for partially encrypting said score.

22. A system as set forth in claim 18, 19, 20, or 21 wherein the source is said network client.

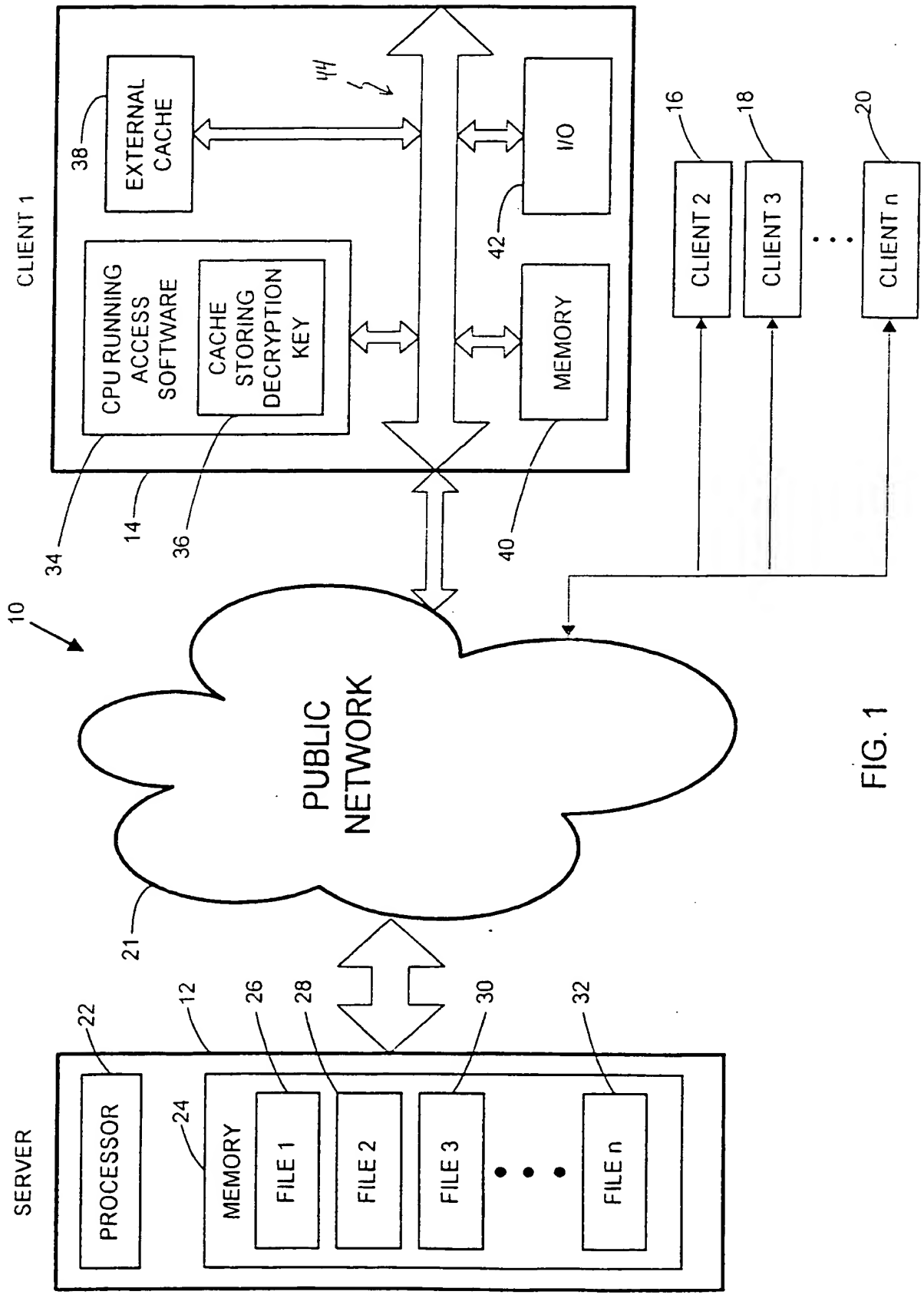

FIG. 1

SYSTEM OVERVIEW

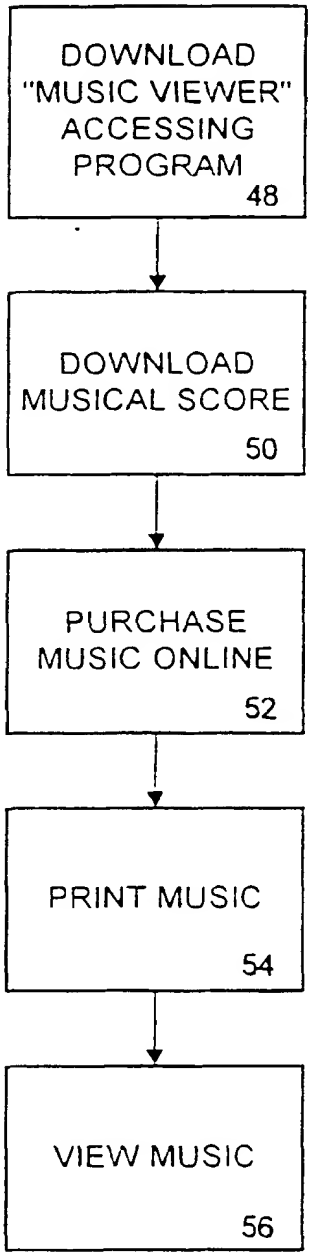

FIG. 2

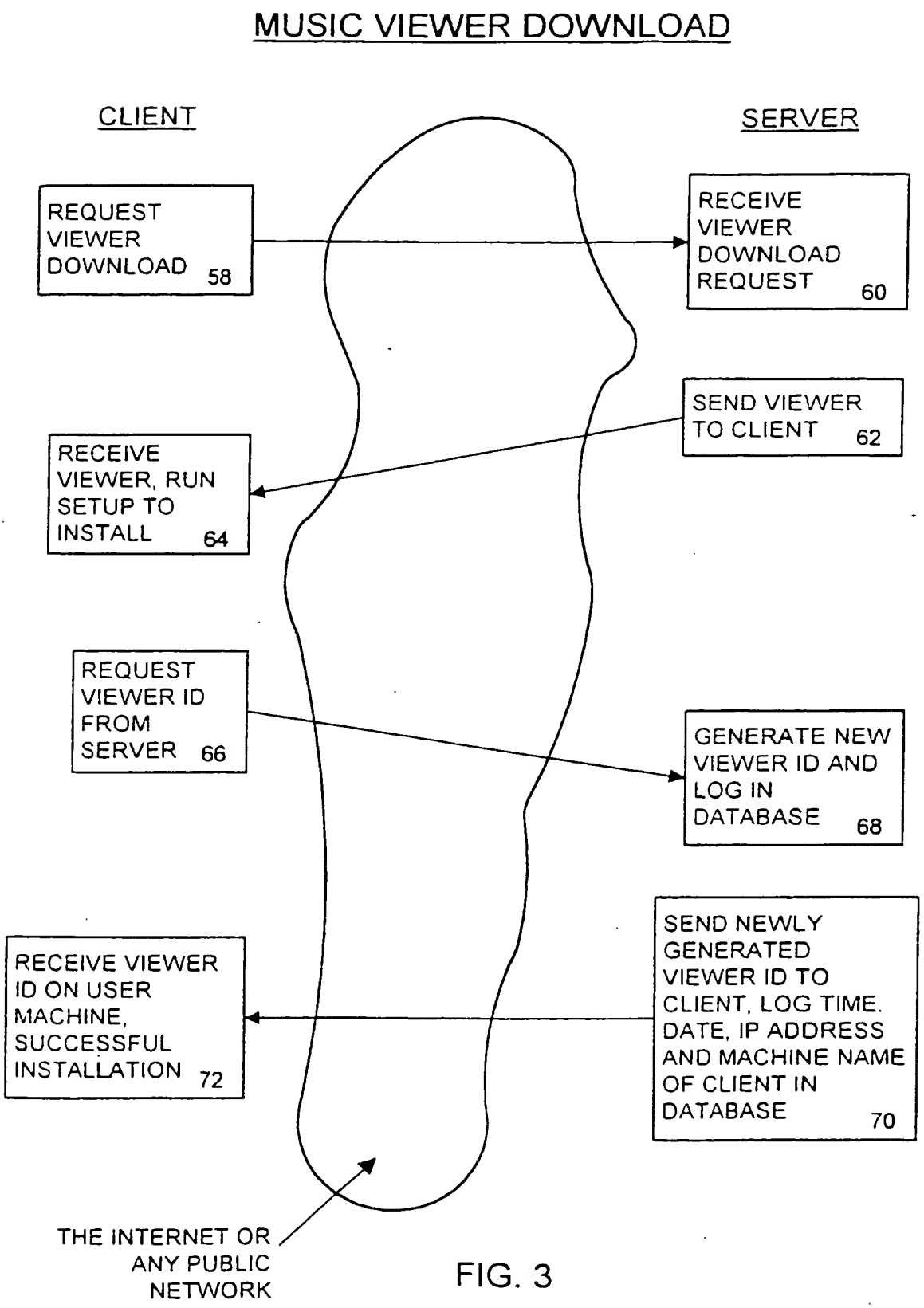

FIG. 3

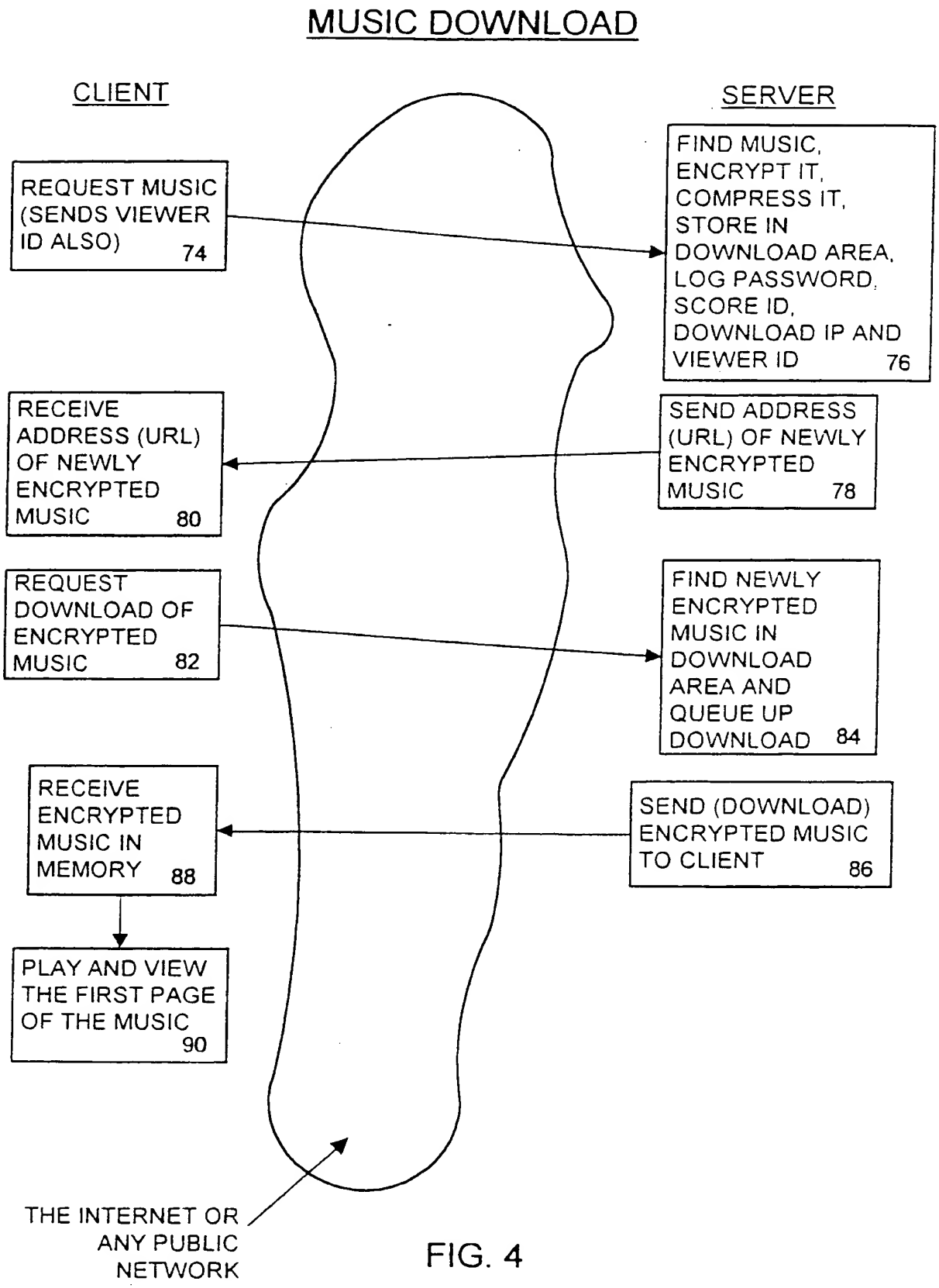

FIG. 4

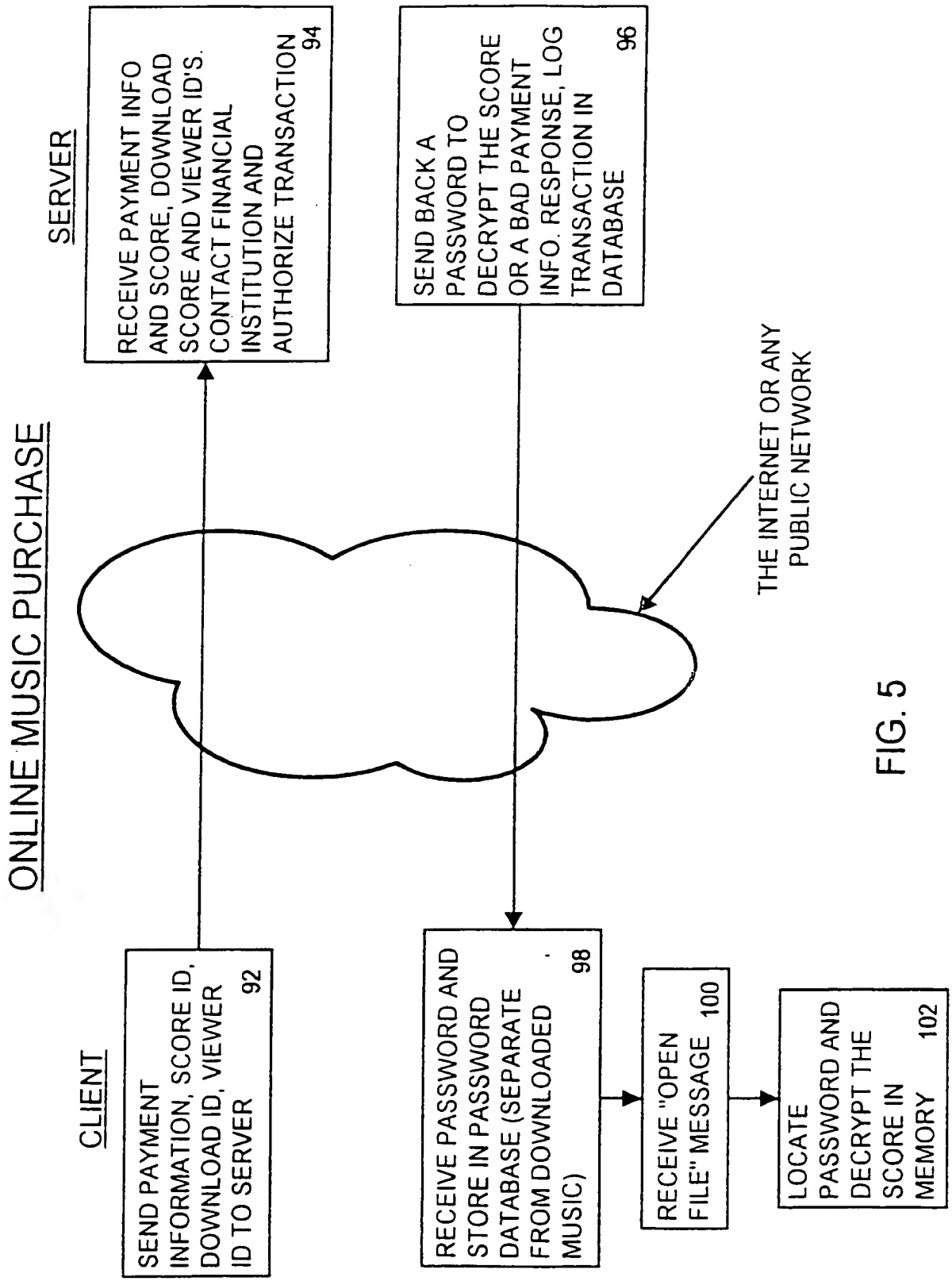
ONLINE MUSIC PURCHASE
CLIENT
SERVER
SEND PAYMENT INFORMATION, SCORE ID, DOWNLOAD ID, VIEWER ID TO SERVER 92
RECEIVE PAYMENT INFO AND SCORE, DOWNLOAD SCORE AND VIEWER ID'S. CONTACT FINANCIAL INSTITUTION AND AUTHORIZE TRANSACTION 94
SEND BACK A PASSWORD TO DECRYPT THE SCORE OR A BAD PAYMENT INFO. RESPONSE, LOG TRANSACTION IN DATABASE 96
THE INTERNET OR ANY PUBLIC NETWORK
RECEIVE PASSWORD AND STORE IN PASSWORD DATABASE (SEPARATE FROM DOWNLOADED MUSIC) 98
RECEIVE "OPEN FILE" MESSAGE 100
LOCATE PASSWORD AND DECRYPT THE SCORE IN MEMORY 102

FIG. 5

PRINTING MUSIC

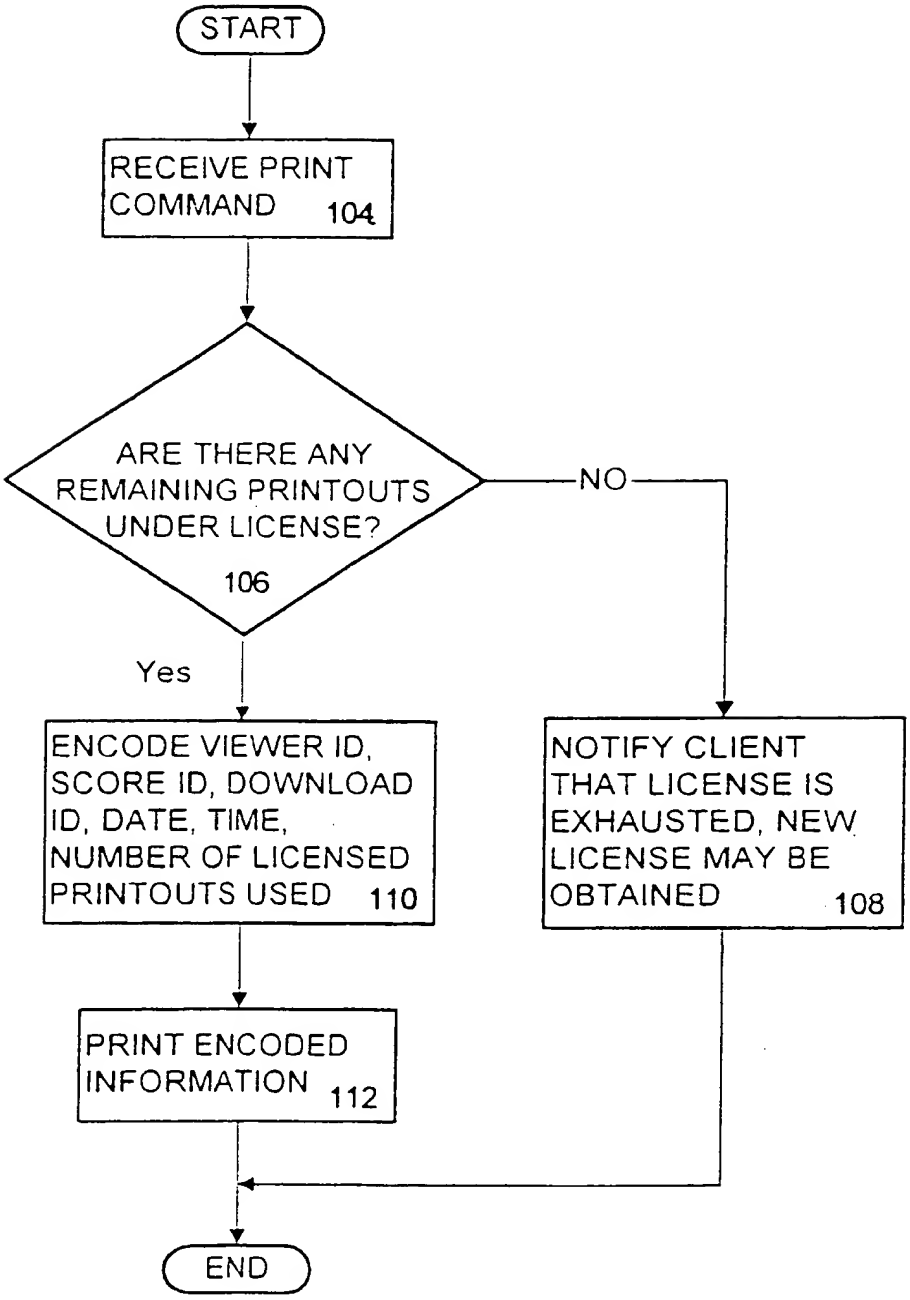

FIG. 6

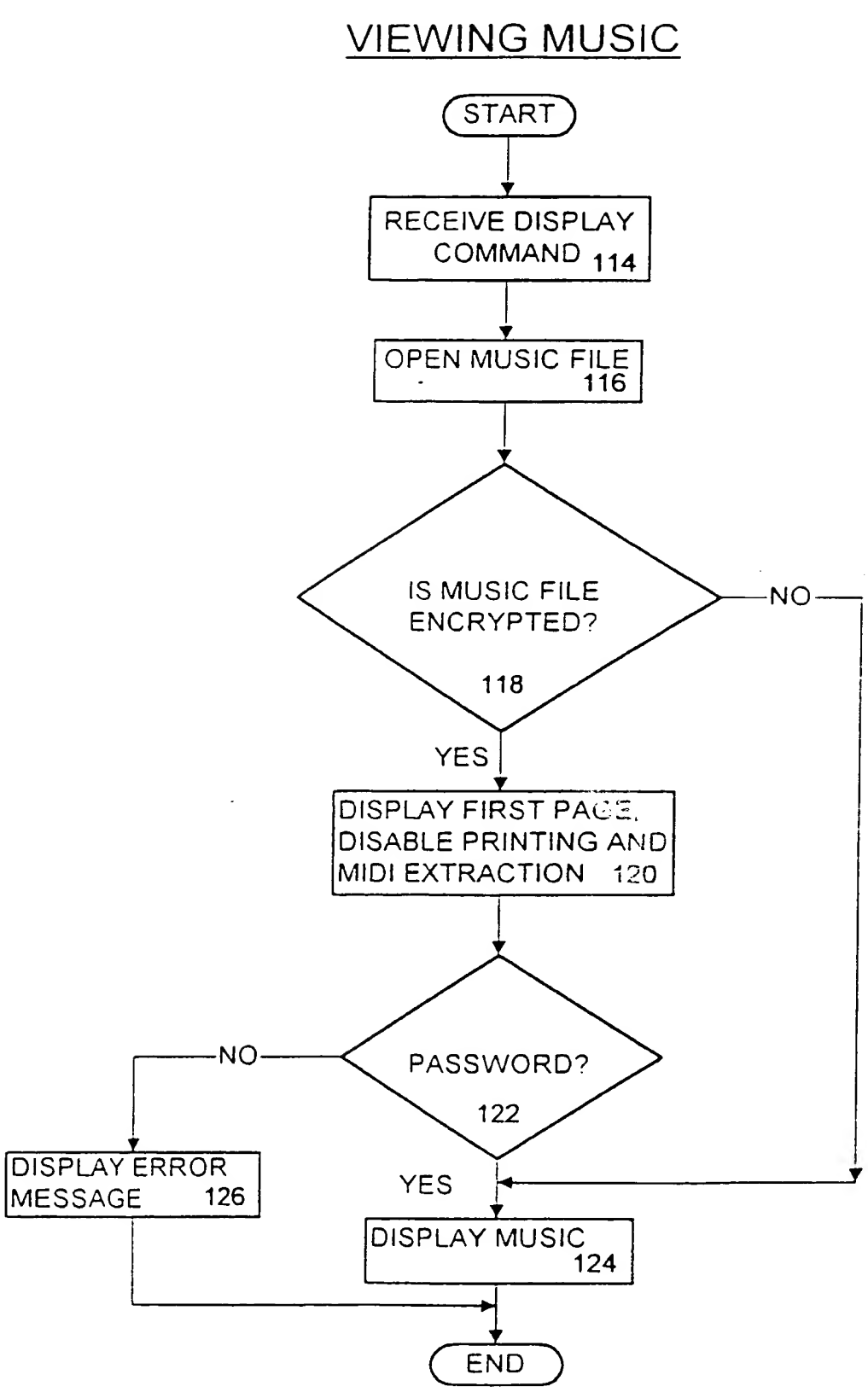
VIEWING MUSIC
START
RECEIVE DISPLAY COMMAND 114
OPEN MUSIC FILE 116
IS MUSIC FILE ENCRYPTED? 118
NO
YES
DISPLAY FIRST PAGE, DISABLE PRINTING AND MIDI EXTRACTION 120
PASSWORD? 122
NO
YES
DISPLAY ERROR MESSAGE 126
DISPLAY MUSIC 124
END

FIG. 7

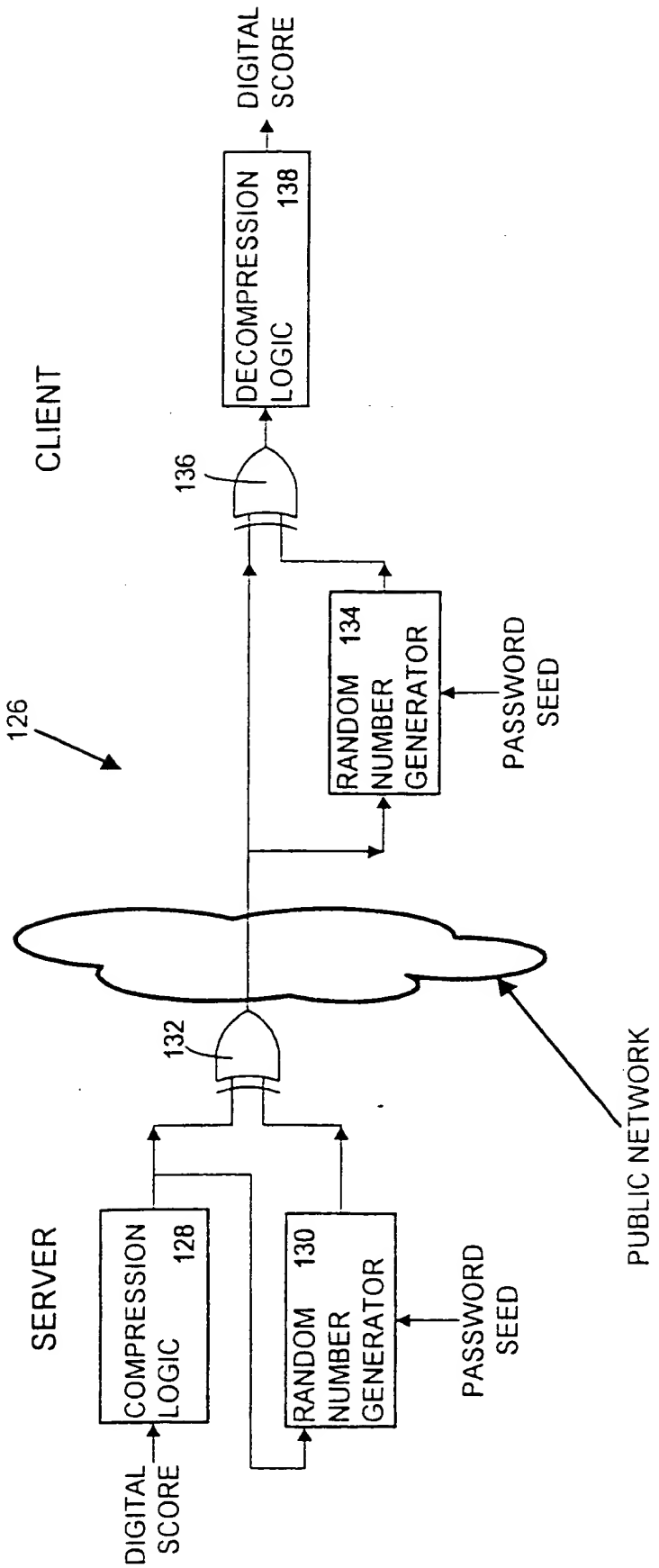

FIG. 8

ENCRYPTION/DECRYPTION

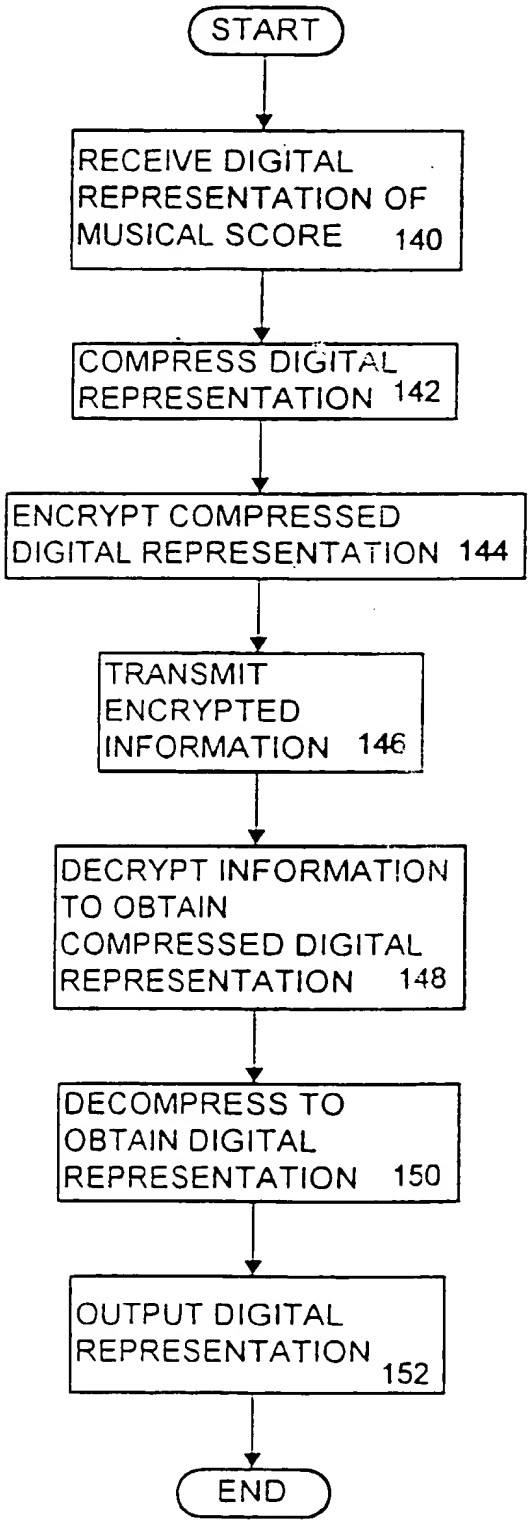

FIG. 9